

REMARKS

This paper is in response to the Office Action of June 14, 2004. The due date for response extends to September 14, 2004.

Claims 12, 14, 20, 22, 23, 24, and 27 have been amended. Claims 1-11 and 28-53 have been cancelled. Claims 54-87 have been added, and are fully supported by the originally filed application and drawings. Claims 12-27 and 54-87 remain pending.

Objection to the informalities:

The objection to the informalities on page 29, line 21 has been corrected by the Preliminary Amendment filed on January 23, 2002.

Objections for claims 36-37 and 44-45:

Because claims 36-37 and 44-45 have been cancelled, the objection is rendered moot.

Rejections under 35 U.S.C. § 102(e):

Since claims 1-11 and 28-53 have been cancelled, the rejections for claims 1-3, 5-11, 28-53 under 35 U.S.C. § 102(e) are rendered moot.

I. Independent claim 12

Claims 12-21 were rejected under 35 U.S.C. § 102(e), as being anticipated by Uranaka et al. (U.S. Patent No. 6,470,085). This rejection is respectfully traversed. As noted in the listing of the claims, certain clarification amendments were made to improve the readability of the claims.

Uranaka defines a system for permitting only an authenticated user to play a desired application contained in an application package. The system has a client for playing the desired application under the control of a server connected with the client through a communication network. The client identifies the server by using a server public key (Pks) that comes with the application package and initiates a service request to the server for playing the desired application. After receiving permission from the server, the client will obtain the application-encrypting key (Kv) that is encrypted by the user public key (Pku). A user secret key (Sku) is obtained from an IC card after the user provides a password. The Sku,

corresponding to the Pku, is used to decrypt the Pku-encrypted Kv. Then, the Kv-encrypted application is decrypted by the Kv.

It is important to note that all four keys (Pks, Pku, Kv, and Sku) are predetermined and none of them are user-specific. Those keys are defined without regard to who the user will be, and will enable any user to gain access provided he or she pays and obtains a password. Essentially, this security is used for transport security and not for securely identifying a user for specific media.

For example, Uranaka does not teach that the detachable storage media have a data structure including a user identifier. Thus, Uranaka fails to teach that a server computer encrypts the software product using the user identifier and a purchase option that governs the use of the software product by the user. In stead, Uranaka teaches to encrypt the distributed application package by the application-encrypting key Kv that is encrypted by the user public key Pku. The user public key Pku is not tied to any particular user, and thus enables distribution of software to any number of random users.

Accordingly, the Applicants respectfully request that the Examiner withdraw the rejection of independent claim 12 under 35 U.S.C. § 102(e).

The Examiner also rejected claims 13-21 under 35 U.S.C. § 102(e) as being anticipated by Uranaka. Claims 13-21, each of which ultimately depends from independent claim 12, are likewise submitted to be patentable under 35 U.S.C. § 102(e) over the Uranaka reference for at least the same reasons set forth above regarding independent claim 12.

II. Independent claim 22

Claims 22-27 were also rejected under 35 U.S.C. § 102(e), as being anticipated by Uranaka et al. (U.S. Patent No. 6,470,085). This rejection is respectfully traversed. As noted in the listing of the claims, certain clarification amendments were made to improve the readability of the claims.

In the system taught by Uranaka, the client does not send any encrypted information to the server; therefore, the server in the cited reference does not perform any decryption function.

Thus, Uranaka fails to teach a server computer that will decrypt the information encrypted by the user. Furthermore, based on the argument set forth for claim 12, Uranaka does not teach or suggest that a server computer has an encryption module for encrypting the software product using the user identifier and the purchase option, which governs the use of the software product by the user.

Accordingly, the Applicants respectfully request that the Examiner withdraw the rejection for claim 22 under 35 U.S.C. § 102(e).

The Examiner also rejected claims 23-27 under 35 U.S.C. § 102(e) as being anticipated by Uranaka. Claims 23-27, each of which ultimately depends from independent claim 22, are likewise submitted to be patentable under 35 U.S.C. § 102(e) over the Uranaka reference for at least the same reasons set forth above regarding independent claim 22.

Rejections under 35 U.S.C. § 103:

Claim 4 was rejected under Section 103. Claim 4 was cancelled in this amendment, and therefore, withdrawal of this rejection is respectfully requested.

Newly added claims 54-87:

Of the newly added claims, claims 54, 65, 74, and 81 are independent claims. Each independent claim and its dependent claims are submitted to be patentable over the cited arts of Uranaka and Richardson III (US Pat. 5,490,216). Claim 54 relates to an overall method for distributing a software product and claim 81 relates to a client console suitable for use on a consumer side. Claim 65 relates to software suitable for use on a content provider server side, whereas claim 74 relates to software suitable for use on a client console side. Each newly added independent claim will be summarized below.

I. Newly added independent Claim 54:

Claim 54 defines a method for distributing a software product. The method includes encrypting said software product and distributing said encrypted software product to a user.

The method further includes establishing two-way, public key/private key encrypted, secure communication between a product distributor and said user. And, communicating, via said secure communication, data (Title B) enabling decryption of said encrypted software product from said product distributor to said user.

II. Newly added independent Claim 65:

Claim 65 defines an article of manufacture that embodies a program of instructions executable by a machine. The program of instructions is configured and adapted for execution on a content provider server. The article of manufacture includes instructions for encrypting a software product, establishing two-way, public key/private key encrypted, secure communication between the content provider server and a client console, in conjunction with a reception of counterpart communication originated from the client console, and communicating data (Title B) via the established secure communication to the client console. The Title B is used for decrypting the encrypted software product.

III. Newly added independent Claim 74:

Claim 74 defines an article of manufacture embodying a program of instructions executable by a machine. The program of instructions is configured and adapted for execution on a client console. The article of manufacture includes instructions for receiving an encrypted software product, establishing two-way, public key/private key encrypted, secure communication between a content provider server and the client console, in conjunction with a reception of counterpart communication originated from the remote content provider server, and receiving data (Title B) via the established secure communication from the content provider server. The Title B is used for decrypting the encrypted software product.

VI. Newly added independent Claim 81:

Claim 81 defines a client console for execution and/or reproduction of a software product. The defined client console includes means configured and adapted for receiving an encrypted software product and means for establishing two-way, public key/private key

encrypted, secure communication between a content provider server and the client console, in conjunction with a reception of counterpart communication originated from the content provider server. The client console further includes means for receiving data (Title B) from the content provider server via the established secure communication. The Title B will enable decryption of the encrypted software product.

* * * *


The newly added independent claims 54, 65, 74, and 81 are supported by the as-filed application, and specifically Figures 2A and 2B and their respective descriptions. Therefore, no new matter is introduced. All four newly added independent claims include the feature of establishing of two-way, public key/private key encrypted, secure communication between a content provider server/product distributor and a client console/user.

In contrast, Uranaka does not teach a method/system with two-way secured communication. Uranaka only teaches a method or a system that has a one-way secured communication, i.e., the contents sent by the server is encrypted, while the contents sent by the client is not encrypted. Further, although Richardson III was cited under Section 103 to reject a cancelled claim, the teachings of Richardson do not overcome the deficiencies of Uranaka, and thus they would not be combinable to establish a valid rejection of the newly added claims.

A Notice of Allowance is therefore respectfully requested.

If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 749-6903. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SONYP005). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE & PENILLA, LLP



Albert S. Penilla, Esq.
Reg. No. 39,487

- 710 Lakeway Drive, Suite 170
Sunnyvale, CA 94085
- Telephone: (408) 749-6900
Facsimile: (408) 749-6901
Customer No. 25920